UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/594,124	09/25/2006	David Roxburgh	LB-36-2015	8934

23117 7590 08/31/2010

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
VU, BAI D	

ART UNIT	PAPER NUMBER
2165	

MAIL DATE	DELIVERY MODE
08/31/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/594,124
Filing Date: September 25, 2006
Appellant(s): ROXBURGH ET AL.

Leonidas Boutsikaris
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 06/15/2010 appealing from the Office action mailed 11/19/2009.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

Claims 2-6, 8 and 16-18.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the

subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner.

The rejection of claims 2-6, 8 and 16-18 under 35 U.S.C. 112, first paragraph.

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

6,510,464 B1	Grantges, Jr. et al.	1-2003
6,763,384 B1	Gupta et al.	7-2004
6,081,906 A	Nishizawa et al.	6-2000
5,935,211	Osterman	8-1999
2005/0050329 A1	Wilding et al.	3-2005

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 8, 16 and 17 are rejected under 35 U.S.C. 103(a) as being anticipated by Grantges, Jr. et al. (US Pat. No. 6,510,464 B1), (hereinafter Grantges), and further in view of Wilding et al. (US Pub. No. 2005/0050329 A1).

As per **claim 16**, Grantges discloses **a system comprising:**

programmed computer devices which execute program code to provide a first sub-system and a gateway for offering services provided by the first sub-system to one or more application hosting sub-systems via the gateway and a data communications network between said gateway and sub-systems; as (see e.g., col. 4 lines 7-19; and Figs. 1-2, as the proxy servers 34 and 40 in Fig. 1 are read on the claimed gateway included notification server 220 in Figure 2; the user 18 of a client computer 22 interpreted as application hosting sub-system; and web servers 28.sub.1, 28.sub.2, . . . , 28.sub.3 interpreted as a first sub-system).

the gateway and each application hosting sub-system being arranged to permit each application hosting sub-system to initiate a secure and authenticated connection from each application hosting sub-system to the gateway as (see e.g., col. 5 line 58 to col. 6 line 2; col. 6 lines 37-40; and Figs. 1-2; as secure connections 52 and 54) **via a non-secure data network connection, and** as (see e.g., Fig. 2, as the insecure network (Internet) 26).

the gateway being logically connected to the first sub-system to enable the services provided by the first sub-system to be provided to each application

hosting sub-system as (see e.g., col. 9 lines 19-35; and Fig. 2, as the "options page" presents a list of authorized applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 for selection by user 18 of client computer 22) **via a secured and authenticated connection,** as (see e.g., Fig. 1; as secure connections 52, 54 and 56).

the gateway including notification means for initiating an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems and transmitting over this or each such connection a notification for notifying said one or more of the application hosting sub-systems that it should initiate a secure authenticated connection with the gateway when the notification means is requested so to do by any one of the services offered by the first sub-system as server (i.e., referred as the first sub-system), through application gateway using an unsecure network, sends "popup" massage displayed "options page" with multiple applications for selection to client computer 22 to establish a secure network connection when the client computer 22 selects a particular application (col. 4 line 36-65; and Fig. 7); the "options page" included applications to be selected in message 78 to client computer 22 via the proxy servers 34 and 40 interpreted as notification of set up an access to the selected applications (see e.g., col. 9 lines 6-24; and Figs. 1-2); and the client computer 22 is authorized to access the selected applications via the proxy servers 34 and 40 (see e.g., Figs. 5-7), wherein the "options page" in message 78 being sent to client computer 22, interpreted as notification means; but may not be specific to the feature of **the gateway including notification means for initiating an unauthenticated and unencrypted connection to one or more of the application**

hosting sub-systems and transmitting over this or each such connection a notification for notifying said one or more of the application hosting sub-systems that it should initiate a secure authenticated connection with the gateway.

However, Wilding et al. discloses the feature of **the gateway including notification means for initiating an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems and transmitting over this or each such connection a notification for notifying said one or more of the application hosting sub-systems that it should initiate a secure authenticated connection with the gateway** which is not explicitly disclosed by Grantges as (see e.g., ¶¶ 0028 – 0040, and Figs. 3A-3B; as the process starting from the step of transmitting Temporary Server Public Key (i.e., interpreted as a notification to verify the authenticated information) from the service gateway 110 to the service client 108 (i.e., interpreted as hosting sub-system) using unsecure connection, until the step of establishing secure, authenticated and encrypted connection between the service gateway 110 and the service client 108).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Wilding et al. teaching of establishing a secure connection into Grantges system in order to direct a client to establish a secure connection with a server across a public network via a service gateway (Wilding et al., Fig. 1 and ¶ 0010 lines 2-4).

As per **claim 17**, Grantges discloses **a method of offering services provided by a first sub-system to one or more application hosting sub-systems via a gateway which includes a notification means for notifying one or more of the application hosting sub-systems that it should initiate a secure authorized connection with the gateway, the gateway and each application hosting sub-system being arranged to permit each application hosting sub-system to initiate a secure and authenticated connection from each application hosting sub-system to the gateway via a non-secure data network connection, and the gateway being logically connected to the first sub-system to enable the services provided by the first sub-system to be provided to each application hosting sub-system via a secured and authenticated connection, the method comprising:**

sending a request from a service wishing to set up a secure and authenticated connection to an application hosting sub-system as server (i.e., referred as the first sub-system), through application gateway using an unsecure network, sends "popup" massage displayed "options page" with multiple applications for selection to client computer 22 to establish a secure network connection when the client computer 22 selects a particular application (col. 4 line 36-65; and Fig. 7), and the "options page" presents a list of authorized applications 24.sub.1, 24.sub.2, . . . , 24.sub.3 interpreted as a service to user 18 of client computer 22 to make a selection (see e.g., col. 9 lines 19-35; and Fig. 2).

However, Wilding et al. discloses the limitations which are not explicitly disclosed by Grantges as following:

that the notification means send a notification to a respective application hosting sub-system to notify it that it should initiate a secure authenticated connection with the gateway; as (see e.g., ¶¶ 0028 – 0029, as transmitting the Temporary Server Public Key from the service gateway 110 to the service client 108 (i.e., interpreted as a notification to verify the authenticated information in order to set up a secure, authenticated and encrypted connection between the service gateway 110 and the service client 108).

initiating from the notification means to the application hosting sub-system an unauthenticated and unencrypted connection and transmitting over this connection the notification for notifying said application hosting sub-system that it should initiate a secure authenticated connection with the gateway; as (see e.g., ¶¶ 0028 – 0040, and Figs. 3A-3B; as the process starting from the step of transmitting Temporary Server Public Key (i.e., interpreted as a notification to verify the authenticated information) from the service gateway 110 to the service client 108 (i.e., interpreted as hosting sub-system) using unsecure connection, until the step of establishing secure, authenticated and encrypted connection between the service gateway 110 and the service client 108).

causing the application hosting sub-system to set up a secure and authenticated connection with the gateway in response to receipt of the notification; and communicating with the initiating service via said connection as (see e.g., ¶ 0040, as establishing secure, authenticated and encrypted connection between the service gateway 110 and the service client 108).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Wilding et al. teaching of establishing a secure connection into Grantges system in order to direct a client to establish a secure connection with a server across a public network via a service gateway (Wilding et al., Fig. 1 and ¶ 0010 lines 2-4).

As per **claim 2**, Grantges discloses **the system according to claim 16 in which the notification takes the form of a non-executable data file** as (see e.g., col. 6 lines 36-39; and col. 9 lines 19-34, as the options page in message 80 interpreted as the non-executable data file).

As per **claim 8**, Grantges discloses **the system according to claim 16, wherein the first sub-system is a backend sub-system which provides services to the gateway,** as (see e.g., col. 4 lines 7-19; and Figs. 1-2, as each application 24.sub.1, 24.sub.2, . . . , 24.sub.3 includes a respective web server 28.sub.1, 28.sub.2, . . . , 28.sub.3) **and wherein the server sub-system acts as a trusted intermediary between each application hosting sub-system and the backend sub-system** as (see e.g., col. 12 line 57 to col. 13 line 3; and Fig. 6, as the trustee provides the user with instructions to access the certificate authority 50 using the user ID/password; and then sends a message 138 to Information Security 48 that contains the information collected from the user 18, including what application(s) are being requested for remote access).

Claims 3, 6 and 18 are rejected under 35 U.S.C. 103(a) as being anticipated by Grantges, in view of Wilding et al., and further in view of Gupta et al. (US Pat. No. 6,763,384 B1).

As per **claim 3**, Grantges and Wilding et al. do not explicitly disclose **the system according to claim 2 in which the notification takes the form of a simple text file containing an extensible Markup Language, XML, document**.

However, Gupta et al. discloses as (see e.g., col. 8 lines 58-66, as notification is sent in XML (eXtensible Markup Language) contained only information regarding the content and structure of a message).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Gupta et al. teaching of notifying end users over a network of the occurrence of an event into Grantges and Wilding et al. systems in order to notify the occurrence of an event by one or more servers to one or more client processes over a communication network (Gupta et al., col. 3 lines 13-15).

As per **claim 6**, Grantges and Wilding et al. do not explicitly disclose **the system according to claim 16 wherein a single notification server receives notifications from plural services and forwards these to plural client application hosting sub-systems**. However, Gupta et al. discloses as (see e.g., col. 4 lines 56-58; col. 8 lines

30-40; and Fig. 3, as a notification server serves multiple application servers and multiple clients).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Gupta et al. teaching of notifying end users over a network of the occurrence of an event into Grantges and Wilding et al. systems in order to notify the occurrence of an event by one or more servers to one or more client processes over a communication network (Gupta et al., col. 3 lines 13-15).

As per **claim 18**, Grantges and Wilding et al. do not explicitly disclose **computer readable storage media containing a program or suite of computer programs for controlling one or more computer processors to carry out the steps of claim 17 during execution of the computer program or suite of programs**. However, Gupta et al. discloses as (see e.g., col. 4 lines 24-42, as a computer program product having a computer usable medium having a computer program embodied therein, for providing notification of the occurrence of an event over a network).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Gupta et al. teaching of notifying end users over a network of the occurrence of an event into Grantges and Wilding et al. systems in order to notify the occurrence of an event by one or more servers to one or more client processes over a communication network (Gupta et al., col. 3 lines 13-15).

Claim 4 is rejected under 35 U.S.C. 103(a) as being anticipated by Grantges, in view of Wilding et al., and further in view of Nishizawa et al. (US Pat. No. 6,081,906 A).

As per **claim 4**, Grantges and Wilding et al. do not explicitly disclose **the system according to claim 16 wherein the notification means is operable to run separate threads for controlling the forwarding of separate notifications to the client application**. However, Nishizawa et al. discloses as (see e.g., col. 5 lines 12-35, as multi -thread RPC processing of the event notification).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Nishizawa et al. teaching of implementing the multi-thread processing with queuing into Grantges and Wilding et al. systems in order to achieve faster response time in sending notifications to clients.

Claim 5 is rejected under 35 U.S.C. 103(a) as being anticipated by Grantges, in view of Wilding et al., and further in view of Osterman (US Pat. No. 5,935,211 A).

As per **claim 5**, Grantges and Wilding et al. do not explicitly disclose **the system according to claim 16, wherein the notification means includes means for permitting each service provided by the first sub-system to specify the number of times which a notification is to be retried in the event of failure to deliver the notification and means for server retrying to deliver the notification up to the**

specified number of times in the event of failure to deliver the notification over the non-secure network.

However, Osterman discloses as (see e.g., col. 7 lines 43-54, as set polling time to every 10 minutes and stop sending if not updated after 25 minutes).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Osterman teaching of providing status information to the client processes into Grantges and Wilding et al. systems in order to provide a technique that permits client processes to reduce the frequency with which they poll the server processes. This, in turn, dramatically reduces the burden on the server process imposed by such polling (Osterman, col. 2 lines 51-54).

(10) Response to Argument

(i) With respect to the appellant's argument about "whether claims 2-6, 8 and 16-18 are unpatentable under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the written description requirement" asserted, on pages 12-14 that independent claims 16 and 17 have support in the instant specification and dependent claims 2-6, 8 and 18 also comply with 35 U.S.C. § 112, first paragraph.

In response to the appellant's argument, the examiner acknowledges the support of the instant specification as provided by appellant on pages 12-14. Therefore, the rejection of claims 2-6, 8 and 16-18 under 35 U.S.C. § 112, first paragraph has been withdrawn.

(ii) With respect to the appellant's argument about "whether independent claims 16 and 17 are obvious under 35 U.S.C. § 103(a) over Grantges (US 6,510,464 B1) in view of Wilding et al. (US 2005/0050329 A1)" asserted, on pages 14-20 that none of the Grantges and Wilding et al. teaches or suggests "the *gateway* including notification means for *initiating* an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems and transmitting over this or each such connection a notification for notifying said one or more of the application hosting sub-systems that *it should initiate a secure authenticated connection with the gateway when the notification means is requested so to do by any one of the services offered by the first sub-system*", emphasis added, as required by claims 16 and 17.

In response to the appellant's argument, the examiner respectfully disagrees because:

First, the connection between the gateway and the application hosting sub-system is already established as the claimed limitation of **the gateway and each application hosting sub-system being arranged to permit each application hosting sub-system to initiate a secure and authenticated connection from each application hosting sub-system to the gateway via a non-secure data network connection**, which is listed prior to the argued limitation **the gateway including notification means for initiating an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems and transmitting over this or each such connection a notification for notifying said one or more of the application hosting sub-systems that it should initiate a secure authenticated connection with the gateway when the notification means is requested so to do by any one of the services offered by the first sub-system** as claimed. Therefore, how can a non-secure connection now be established? The connection is already secured.

Second, Grantges discloses **the gateway including notification means for initiating an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems and transmitting over this or each such connection a notification for notifying said one or more of the application hosting sub-systems that it should initiate a secure authenticated connection with the gateway when the notification means is requested so to do by any one of the**

services offered by the first sub-system as server (i.e., referred as the first sub-system), through application gateway using an unsecure network, sends "popup" massage displayed "options page" with multiple applications for selection to client computer 22 to establish a secure network connection when the client computer 22 selects a particular application (col. 4 line 36-65; and Fig. 7); the "options page" included applications to be selected in message 78 to client computer 22 via the proxy servers 34 and 40 interpreted as notification of set up an access to the selected applications (see e.g., col. 9 lines 6-24; and Figs. 1-2); and the client computer 22 is authorized to access the selected applications via the proxy servers 34 and 40 (see e.g., Figs. 5-7), wherein the "options page" in message 78 being sent to client computer 22, interpreted as notification means; but may not be specific to the feature of **the gateway including notification means for initiating an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems and transmitting over this or each such connection a notification for notifying said one or more of the application hosting sub-systems that it should initiate a secure authenticated connection with the gateway.** As it is well known in the telecommunication technology, all "communicating" devices in a network send a pulse/beat to each other to make sure of the availability for further communication therefore the "options list" devices are established devices that share the same communication network.

However, Wilding et al. discloses the feature of **the gateway including notification means for initiating an unauthenticated and unencrypted connection**

to one or more of the application hosting sub-systems and transmitting over this or each such connection a notification for notifying said one or more of the application hosting sub-systems that it should initiate a secure authenticated connection with the gateway which is not explicitly disclosed by Grantges as (see e.g., ¶¶ 0028 – 0040, and Figs. 3A-3B; as the process starting from the step of transmitting Temporary Server Public Key (i.e., interpreted as a notification to verify the authenticated information) from the service gateway 110 to the service client 108 (i.e., interpreted as hosting sub-system) using unsecure connection, until the step of establishing secure, authenticated and encrypted connection between the service gateway 110 and the service client 108).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Wilding et al. teaching of establishing a secure connection into Grantges system in order to direct a client to establish a secure connection with a server across a public network via a service gateway (Wilding et al., ¶ 0010 lines 2-4; and Fig. 1).

The claims in general are not clear on the order of communication nor are they clear on the novelty being claimed therefore they are given the broadest reasonable interpretation.

(**iii**) With respect to the appellant's argument about "whether dependent claim 5 is obvious under 35 U.S.C. § 103(a) over Grantges, in view of Wilding et al., and further in view of Osterman (US 5,935,211 A)" asserted, on pages 20-21 that Osterman fails to

cure the deficiency of Grantges/Wilding et al., namely the lack of teaching of initiation by the gateway, and does not discloses the limitation of dependent claim 5.

In response to the appellant's argument, the examiner respectfully disagrees because Grantges in view of Wilding et al. discloses "the gateway including notification means for initiating an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems and transmitting over this or each such connection a notification for notifying said one or more of the application hosting sub-systems that it should initiate a secure authenticated connection with the gateway when the notification means is requested so to do by any one of the services offered by the first sub-system" as clearly discussed above. Furthermore, Osterman discloses the limitation of claim 5 as addressed in the office action above. Therefore, the rejection of claim 5 as being obvious over the teaching of Grantges, in view of Wilding et al., and further in view of Osterman is hereby maintained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Bai D. Vu/

Examiner, Art Unit 2165

8/25/2010

Conferees:

Neveen Abel-Jalil

/Neveen Abel-Jalil/

Supervisory Patent Examiner, Art Unit 2165

Hassan (Tony) Mahmoudi
/Tony Mahmoudi/
Supervisory Patent Examiner, Art Unit 2169